(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 446 974**

(51) Int. CI.:

B60R 25/04 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **08.02.2011 E 11153725 (4)**

(97) Fecha y número de publicación de la concesión europea: **15.01.2014 EP 2484564**

(54) Título: **Método y aparato para la seguridad de vehículos**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.03.2014

(73) Titular/es:

DELPHI TECHNOLOGIES HOLDING S.À.R.L. (100.0%)
Avenue de Luxembourg
4940 Bascharage, LU

(72) Inventor/es:

BURIKS, ADRIAN y
LAMB, RODNEY

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y aparato para la seguridad de vehículos

Campo de la invención

La invención se refiere a métodos y aparatos para la seguridad de vehículos. De manera más específica, la invención se refiere a la seguridad de los datos almacenados en los sistemas informáticos del vehículo.

Antecedentes de la invención

Los vehículos que incluyen un motor de combustión interna incluyen típicamente sistemas informáticos importantes para el funcionamiento efectivo del vehículo. Uno de estos sistemas importantes es una unidad de control de motor (ECU, *Engine Control Unit*). Se trata de una unidad de control electrónico que controla el funcionamiento del motor y configura varios parámetros de funcionamiento, tales como la mezcla y composición del combustible, el ajuste de encendido, la velocidad de ralentí y el control y el reglaje de las válvulas.

Una ECU puede estar equipada con funciones de seguridad para garantizar que no puede ser objeto de una modificación no autorizada - si se detecta una modificación tal, la ECU puede estar adaptada para impedir o de otro modo limitar el funcionamiento del motor. Tales funciones de seguridad se proporcionan en el propio software en diseños de ECU existentes, debido a que el coste adicional y la complejidad del hardware seguro impide que esto pueda ser una solución aceptable en este contexto desde el punto de vista comercial. Tales funciones de seguridad de software están abiertas a ataques mediante la modificación de los datos de la ECU, la reprogramación de la ECU o la sustitución física de la ECU. Esto pone en riesgo la seguridad global del vehículo, ya que estas estrategias pueden utilizarse como una táctica para adquirir el control ilícito de un vehículo.

El documento US2009022317 describe un sistema en el que un dispositivo de recepción que posee funciones de una unidad de control de motor interacciona con una llave inmovilizadora. Este sistema está orientado a la prevención de ataques llevados a cabo clonando la llave inmovilizadora mediante la lectura de claves encriptadas almacenadas en memorias no volátiles. Proporciona a la ECU una memoria FeRAM garantizada contra falsificaciones y proporciona un mecanismo para permitir el borrado de claves almacenadas en la memoria FeRAM después de su uso.

Es deseable proporcionar una solución que evite los riesgos para la seguridad de un vehículo basados en puentear las funciones de seguridad de la ECU.

Resumen de la invención

Por consiguiente, la invención proporciona un método para hacer seguro un vehículo, que comprende: proporcionar una unidad de control de motor, donde un elemento de datos digitales estáticos o más de uno se almacenan en una primera memoria para ser utilizados por la unidad de control de motor; y proporcionar un inmovilizador, donde el inmovilizador proporciona un certificado raíz de confianza para la unidad de control de motor de modo que el inmovilizador está adaptado para asegurar que el elemento o los elementos almacenados en la primera memoria están protegidos contra una modificación no autorizada; donde la unidad de control de motor está adaptada para impedir el funcionamiento, o para limitar el rendimiento, del vehículo a no ser que se lleve a cabo de manera satisfactoria una rutina de validación, donde el mencionado elemento o los mencionados elementos comprenden elementos de datos estáticos utilizados por la rutina de validación y donde los mencionados elementos de datos estáticos comprenden un conjunto de una clave pública o varias de una pareja de claves o conjunto de claves, donde la clave pública o las claves públicas se utilizan en la rutina de validación para determinar si los valores medidos del software de la unidad de control de motor corresponden a los valores firmados utilizando una clave privada asociada o varias.

Esta estrategia evita tipos de actividad que ponen en riesgo la seguridad del vehículo o que modifican su rendimiento mediante la modificación de la ECU o mediante un ataque sobre ella. Utilizando el inmovilizador - que por su función está diseñado para ser un componente relativamente seguro adaptado para ser confiable para el usuario - para garantizar la seguridad de la primera memoria, se sitúa el certificado raíz de confianza para el funcionamiento de la ECU en el inmovilizador, lo que mejora la seguridad del vehículo y la confianza del usuario. Los inmovilizadores son elementos necesarios en muchas jurisdicciones, y se construirán de acuerdo con estándares de seguridad lo suficientemente altos como para conseguir un funcionamiento efectivo y lograr un alto nivel de certificación (por ejemplo, para reducir primas de seguro) ya que su utilización de esta manera aumentará previsiblemente la seguridad global del sistema.

En una implementación, el inmovilizador comprende la primera memoria, de modo que si se lleva a cabo un intento de modificar o retirar datos en la primera memoria, el inmovilizador proporciona una respuesta de inmovilización para evitar el funcionamiento efectivo del vehículo. Para ayudar en esta tarea, el elemento o los elementos pueden almacenarse en forma encriptada y/o la memoria del inmovilizador puede estar protegida físicamente contra modificaciones.

En una implementación alternativa, la primera memoria está comprendida dentro de la unidad de control de motor, de modo que el inmovilizador comprueba la primera memoria para determinar si un valor del elemento o de los elementos almacenados en ella son válidos, de manera que si cualquier valor resulta no ser válido, el inmovilizador proporciona una respuesta de inmovilización para evitar el funcionamiento efectivo del vehículo.

Esta estrategia puede implementarse con facilidad mediante modificaciones ligeras a ECUs existentes y a diseños de inmovilizadores, y consigue un resultado fidedignamente seguro.

La primera memoria puede estar comprendida dentro de la memoria flash de la unidad de control de motor. En esta disposición, el elemento o los elementos pueden almacenarse en forma encriptada y pueden ser desencriptados mediante interacción con el inmovilizador.

La unidad de control de motor está adaptada para restringir el funcionamiento del vehículo a no ser que se lleve a cabo una rutina de validación de manera satisfactoria, en cuyo caso el elemento o los elementos pueden comprender elementos de datos estáticos utilizados por la rutina de validación. El inmovilizador puede ser por lo tanto utilizado para asegurar la autenticidad de parámetros utilizados en cualquier tipo de validación segura de la ECU y sus comunicaciones. El elemento o los elementos comprenden una clave pública o varias de un conjunto de claves de encriptación asimétrica, donde una clave pública o varias se utilizan en la rutina de validación para determinar si los valores medidos del software de la unidad de control de motor o los datos comunicados a la ECU corresponden a valores firmados por las correspondientes claves privadas. Éstas claves pueden por ejemplo estar en una pareja de claves, o pueden estar en un esquema de firma de grupo. Como ejemplo adicional, los valores pueden ser un conjunto de uno o varios valores hash más seguros dentro de la ECU utilizados para validar el software o la integridad de los datos. Podrían utilizarse soluciones criptográficas alternativas, y también parámetros relevantes protegidos según la estrategia descrita aquí.

El elemento de datos o los elementos de datos pueden comprender código para ser ejecutado por un procesador de la unidad de control de motor o bien valores estáticos de la unidad de control de motor, o ambos. Esto puede estar enteramente separado del esquema de validación (relacionado con otro código utilizado conjuntamente en el funcionamiento de la unidad de control de motor), pero para el esquema de validación esto también puede permitir otros valores significativos - tales como claves públicas, valores hash, restricciones de intervalo de memoria, valores hash firmados digitalmente, y/o firmas digitales que deben conservarse de forma segura.

En un aspecto adicional, la invención proporciona un sistema de control de motor para un vehículo, que comprende: una unidad de control de motor, donde un elemento de datos digitales estáticos o más de uno están almacenados en una primera memoria para ser utilizados por la unidad de control de motor; y un inmovilizador, donde el inmovilizador proporciona un certificado raíz de confianza para la unidad de control de motor de modo que el inmovilizador está adaptado para asegurar que el elemento o los elementos almacenados en la primera memoria están protegidos contra una modificación no autorizada; donde la unidad de control de motor está adaptada para restringir el funcionamiento del vehículo a no ser que se lleve a cabo de manera satisfactoria una rutina de validación, donde el mencionado elemento o los mencionados elementos comprenden elementos de datos estáticos utilizados por la rutina de validación, y donde los mencionados elementos de datos estáticos comprenden una clave pública o varias de una pareja de claves o un conjunto de claves, donde la clave pública o las claves públicas se utilizan en la rutina de validación para determinar si los valores medidos del software de la unidad de control de motor corresponden a los valores firmados utilizando una clave privada asociada o más de una.

En una implementación, la primera memoria está comprendida dentro del inmovilizador.

En otra implementación, la primera memoria está comprendida dentro de la unidad de control de motor, de modo que el inmovilizador está adaptado para comprobar la primera memoria para determinar si un valor del elemento o los elementos almacenados en ella son válidos, de modo que si cualquier valor resulta no ser válido, el inmovilizador está adaptado adicionalmente para proporcionar una respuesta de inmovilización para evitar el funcionamiento efectivo del vehículo.

Descripción de realizaciones específicas

Se describirán a continuación realizaciones de la invención, a modo de ejemplo, haciendo referencia a los dibujos que acompañan, en los cuales:

La Figura 1 ilustra de manera esquemática elementos relevantes de un sistema de vehículo;

La Figura 2 ilustra de manera esquemática la relación entre un inmovilizador y una unidad de control de motor de acuerdo con una realización de la invención; y

La Figura 3 ilustra de manera esquemática un método de funcionamiento del inmovilizador con respecto a la unidad de control de motor de acuerdo con una realización de la invención.

La Figura 1 muestra elementos relevantes de un sistema de vehículo típico. El motor 1 del vehículo funciona bajo el control de una unidad 2 de control de motor (ECU) en un que controla el funcionamiento del motor y configura varios

parámetros de funcionamiento del motor 1. La ECU 2 interacciona con otros elementos del vehículo, enlazada mediante la red y el sistema eléctrico del vehículo, y entre estos elementos se encuentra el inmovilizador 3. El inmovilizador 3 es un dispositivo electrónico que desactiva el funcionamiento efectivo del vehículo a no ser que esté presente el testigo de autenticación correcto. Este testigo de autenticación es proporcionado generalmente mediante una llave 4 física portada por el conductor del vehículo (la llave del vehículo del conductor).

La ECU 2 está implementada generalmente como una placa de circuito que comprende una CPU 5 y una memoria 6 o más de una junto con otros componentes electrónicos. El software para el funcionamiento de la ECU 2 está almacenado típicamente dentro de esta memoria 6 (alguna parte también puede estar presente dentro de una memoria dedicada dentro de la propia CPU 5). Típicamente, la memoria 6 comprende memoria flash o memorias EPROM. La CPU 5 puede por lo tanto ser generalmente reprogramada mediante la sustitución del software instalado en la memoria 6 (posiblemente también mediante la adición de circuitos integrados adicionales para proporcionar funcionalidades específicas).

Un inmovilizador 3 es un componente estándar de un vehículo, y en muchas jurisdicciones el uso de un inmovilizador para protegerse contra el uso no autorizado o el robo es obligatorio (y en otras jurisdicciones determinará las primas de seguro). Muchos inmovilizadores existentes aplican algoritmos criptográficos para garantizar la autenticidad de componentes físicos del vehículo tales como la llave 4 del vehículo. Si la autenticación del componente falla, los inmovilizadores desactivarán el funcionamiento efectivo del vehículo.

El inmovilizador 3 puede utilizar una variedad de estrategias diferentes para desactivar el funcionamiento efectivo del vehículo. El inmovilizador 3 utilizará una de estas estrategias o más de una como parte de una respuesta de inmovilización cuando se detecta una condición de disparo (tal como un intento de activar el vehículo sin el testigo de autenticación correcto). Las estrategias utilizadas varían dependiendo del diseño específico del inmovilizador utilizado y de los sistemas presentes dentro del vehículo. En algunos casos, el inmovilizador 3 utiliza partes de la memoria 6 de la ECU e interacciona con la ECU 2 para evitar el funcionamiento del motor 1, como por ejemplo haciendo que la ECU 2 evite que fluya combustible o que se produzca la ignición. Aunque las realizaciones de la invención implican la interacción entre la ECU 2 y el inmovilizador 3, debería apreciarse que las realizaciones de la invención no necesitan que esto ocurra como parte de la respuesta normal de inmovilización del inmovilizador 3 para desactivar el funcionamiento efectivo del vehículo cuando se detecta una condición de disparo.

La interacción entre la llave 4 y el inmovilizador 3 es típicamente del tipo siguiente. El testigo de autenticación dentro de la llave 4 comprende un valor almacenado en una memoria particular. Cuando se inserta en el sitio adecuado dentro del vehículo, el valor almacenado se transmite al inmovilizador 3. Esto puede llevarse a cabo según un número de maneras alternativas. Una manera consiste simplemente en realizar una conexión eléctrica directa entre las partes relevantes de la llave y el inmovilizador. Una estrategia preferida consiste en almacenar el valor en una etiqueta RFID dentro de la llave 4. Esta etiqueta es activada, y el valor es emitido y detectado por el inmovilizador 3 o por algún otro elemento en su lugar cuando la llave se sitúa en la posición apropiada en el vehículo. Si el valor almacenado es el esperado por el inmovilizador 3, se permite el funcionamiento del vehículo, mientras que en caso contrario se dispara la respuesta de inmovilización.

Para determinar si el valor almacenado es el valor esperado, algunos diseños del inmovilizador 3 pueden utilizar la memoria 6 de la ECU. El valor correcto (y por tanto esperado) puede almacenarse en un área dedicada de la memoria 6 de la ECU. El inmovilizador 3 también puede acceder a la ECU 2 y a la memoria 6 de la ECU al llevar a cabo una respuesta de inmovilización, como por ejemplo al evitar que la ECU 2 permita la activación de la bomba de combustible o la ignición.

Los valores esperados y por lo tanto almacenados pueden cambiar a lo largo del tiempo para aumentar la seguridad de este sistema. El valor puede cambiarse entre una interacción y otra mediante el uso de un sistema de código variable o mediante el uso de una solución criptográfica avanzada tal como una libreta de un solo uso. Esto puede requerir una capacidad criptográfica (tal como un procesador criptográfico y una memoria segura) dentro del propio inmovilizador, o bien esta capacidad puede proporcionarse en un componente diferente accesible por el inmovilizador.

La Figura 2 ilustra de manera esquemática la relación entre el inmovilizador 3 y la ECU 2 en una realización de la invención. En esta realización, la ECU 2 utiliza un esquema de firma digital para garantizar que el software utilizado en la ECU 2 es el mismo que proporcionó el fabricante o de otro modo que es un software autorizado. Esto puede conseguirse generando una firma digital de un código específico y almacenando esta información dentro de la memoria 6 de la ECU durante la fabricación. La generación de la firma tiene lugar utilizando una clave privada confiable (tal como la clave privada utilizada por el fabricante para este propósito, y no revelada a otras personas) y el almacenamiento tanto del software como de la firma digital permite la medida subsiguiente. Una clave privada es parte de una pareja de claves cuya autenticidad se garantiza utilizando prácticas consideradas como adecuadamente seguras para el escenario específico. Por ejemplo, la autenticidad de la pareja de claves puede garantizarse utilizando un esquema de firma digital basado en PKI convencional, una web de confianza, o una implementación de otras protecciones físicas y protocolos de seguridad que aseguren la autenticidad a la vez que evitan la divulgación de la clave privada. En otras realizaciones pueden utilizarse disposiciones diferentes - por ejemplo, puede utilizarse un esquema de firma de grupo en el que más de una parte tiene derechos de firma sobre

toda la ECU o parte de ella. En este caso, puede que no haya una relación simple uno-a-uno entre una clave privada y una clave pública - pueden existir múltiples claves privadas asociadas con una única clave pública, o múltiples claves públicas asociadas con una única clave privada.

Una clave 21 pública o varias, que corresponde o corresponden a una clave privada o a varias, se almacena entonces de tal manera que resulte accesible para la ECU 2, típicamente en una parte dedicada de la memoria 6 de la ECU. Antes de actuar bajo una solicitud para llevar a cabo operaciones restringidas (tales como reprogramar una ECU o arrancar un vehículo), la ECU 2 puede utilizar una clave pública o varias y algoritmos de validación de firma digital para validar la autenticidad del software y los datos disponibles para que la ECU 2 implemente la acción. Para el software y los datos almacenados en la ECU, la validación de la firma involucra a firmas digitales almacenadas en la ECU tal como se muestra en el elemento 22 de la Figura 2. Antes de actuar bajo una solicitud comunicada a la ECU, pueden utilizarse una clave pública y un algoritmo de validación de firma digital para verificar que la solicitud, el software y los datos recibidos por un canal de comunicación son auténticos. En este caso, el mensaje, y no la ECU, contendrá típicamente la firma digital utilizada para la validación. En los dos escenarios, si la información digital no se considera auténtica, la ECU 2 lleva a cabo una acción apropiada (que puede incluir reducir el rendimiento del motor, inhibir la ignición o el funcionamiento de la bomba de combustible o limitar de otro modo la funcionalidad del vehículo).

Esta estrategia puede subvertirse al menos de dos maneras. Una manera consiste en reemplazar la ECU 2 completa. Si se hace esto, se puenteará todo el esquema de firma digital. Otra manera consiste en reemplazar una clave pública o varias y las firmas digitales con claves públicas y firmas digitales nuevas cuando se modifica el software de la ECU. La nueva clave pública o las nuevas claves públicas son parte de conjuntos de claves no autorizados, estando una clave privada o varias de cada conjunto en poder del modificador. El modificador utiliza una clave privada ilícita para generar firmas del software de la ECU modificado, y estas nuevas firmas digitales son grabadas para reemplazar las firmas originales. Aunque el algoritmo de validación de firma digital utilizado por la ECU no ha sido modificado y continúa funcionando exactamente como lo hacía antes, no detectará el acto de subversión. Esto escapa a la detección porque a pesar de que la ECU 2 puede aplicar un algoritmo de verificación de firma digital para garantizar que los datos han sido firmados con una clave privada o varias que corresponden a las claves públicas disponibles para el algoritmo, la ECU 2 es incapaz de garantizar que sus propias claves públicas son auténticas. En el mundo de los ordenadores interconectados en red, este problema se resuelve habitualmente mediante comunicaciones con una tercera parte confiable para establecer la autenticidad de las claves, como por ejemplo contactando con una autoridad certificadora remota que sea parte de una PKI. Un mecanismo tal no está disponible en la mayor parte de las ECUs y su implementación aumenta los costes económicos. Por lo tanto, los datos internos de la ECU, típicamente las claves públicas y los certificados almacenados dentro de la propia ECU, sirven comúnmente como el certificado raíz de confianza para tales dispositivos embebidos, y deben ser protegidos.

Pueden conseguirse algunas medidas de seguridad almacenando estos valores sensibles en una memoria dedicada o segura (tal como la memoria de un módulo de plataforma confiable (TPM, *Trusted Platform Module*) garantizada frente a falsificaciones) o mediante encriptación adicional (por ejemplo, basada en un número de identificación de ECU único), pero esto añade un coste económico significativo y puede no resultar efectivo contra una sustitución total de la ECU.

La Figura 2 muestra cómo realizaciones de la invención evitan estos tipos de subversión. El inmovilizador 3 interacciona con la ECU 2 de manera normal, pero también asume la responsabilidad sobre ciertos elementos de los datos estáticos dentro de la memoria de la ECU 2. En el caso considerado específicamente aquí, esto puede implicar la asunción de la seguridad de las claves 21 públicas del software de validación de firma digital de la ECU, y posiblemente también de otros valores estáticos del sistema ECU (tales como, por ejemplo, valores hash seguros) aunque otros valores estáticos significativos para el funcionamiento de la ECU también pueden almacenarse de esta manera). Otros datos estáticos pueden protegerse de la misma manera, tales como código utilizado por la ECU en funcionamiento (esto puede ocurrir durante el funcionamiento normal de la ECU y no sólo durante el funcionamiento del esquema de firma digital). Sin embargo, puesto que el inmovilizador 3 tiene la responsabilidad sobre datos que se necesitan para el funcionamiento del esquema de firma digital, ni la sustitución de la ECU ni tampoco la sustitución del esquema de firma digital de la ECU cuando se reemplaza el software serán efectivos sin que también se produzca la subversión o la sustitución del inmovilizador 3. Conseguir esto puede resultar más problemático, debido a que puesto que la función básica del inmovilizador consiste en proteger el vehículo, estará generalmente bien protegido contra un ataque físico o contra otra subversión. Moviendo el certificado raíz de confianza desde la relativamente insegura ECU 2 hasta un dispositivo seguro, el inmovilizador 3, el coste para un atacante de la modificación de valores críticos para subvertir las medidas de seguridad aumenta. Esto conduce a una menor frecuencia de ataques y a una seguridad del vehículo mejorada.

La cantidad de memoria disponible para el inmovilizador 3 y el camino de comunicación entre el inmovilizador 3 y la ECU 2 puede determinar la cantidad de datos protegidos. Esto también puede determinar si un elemento de datos está protegido mediante la protección del propio elemento de datos en el inmovilizador (más seguro pero que necesita más espacio) o mediante el almacenamiento de una firma digital o de un hash seguro del elemento de datos (posiblemente menos seguro y que requiere un procesado adicional, pero menos necesitado de memoria).

Son posibles otras estrategias alternativas para la protección de estos valores por parte del inmovilizador 3. El

inmovilizador 3 puede simplemente almacenar estos valores en una memoria 25 del inmovilizador, y la ECU 2 puede obtenerlos del inmovilizador 3 cuando se necesite bien directamente desde la memoria 25 del inmovilizador (siempre y cuando la ECU 2 no sea capaz de escribir en esta memoria) o bien mediante solicitud a un procesador 26 del inmovilizador - intentos de obtener estos valores de una manera diferente a la aprobada dispararían una respuesta de inmovilización. Alternativamente, el inmovilizador 3 puede contener una firma digital o un hash seguro de estos valores en una memoria 25 del inmovilizador, y el procesador 26 del inmovilizador puede utilizar un algoritmo de validación para determinar si estos valores 25 corresponden a aquellos calculados a partir del código almacenado en la memoria 6 de la ECU. Si la validación y estos valores no son considerados auténticos, se adoptaría una respuesta de inmovilización. Este hash almacenado también puede ser una firma digital para la cual el inmovilizador 3 posee una clave pública - de esta manera, el propio esquema de firma digital para la ECU 2 estaría asegurado mediante un esquema de firma digital.

Si está dotado de capacidades criptográficas, bien a través del software interno o bien mediante la inclusión de un co-procesador criptográfico y una memoria segura (que puede estar presente en algunas soluciones de inmovilizador con el fin de proporcionar un alto nivel de seguridad entre el inmovilizador 3 y la llave 4 o la ECU 2), más soluciones criptográficas avanzadas estarán entonces disponibles. Por ejemplo, podrían generarse parejas de claves y firmas digitales de corta duración para permitir la protección de datos dinámicos.

El papel del inmovilizador consiste en asegurar que se cumplen un cierto número de precondiciones antes de permitir un funcionamiento normal. Estas precondiciones pueden testearse en un orden en serie o en paralelo dependiendo de los requerimientos de diseño y las capacidades del hardware. El orden en el que se llevan a cabo los test puede variar entre implementaciones. La Figura 3 ilustra la realización preferida de un proceso serie para el funcionamiento del inmovilizador 3 cuando la llave 4 se sitúa en posición. El inmovilizador determina primero en el paso 31 si la llave 4 proporciona un testigo de autenticación válido y, si no es así, disparará una respuesta 40 de inmovilización. El inmovilizador comprueba entonces en el paso 32 la clave pública del esquema de firma digital de la ECU (y cualesquiera otros valores estáticos protegidos por el inmovilizador) y de nuevo si la comprobación falla esto disparará una respuesta 40 de inmovilización. La ECU comprueba entonces en el paso 33 los valores de software utilizando el esquema de firma digital de la ECU y, si estas comprobaciones fallan, la ECU no permitirá el funcionamiento del vehículo (o incluso puede ella misma disparar una respuesta de inmovilización) - en caso contrario se permite en el paso 34 el funcionamiento normal del vehículo.

Este uso cooperativo del inmovilizador y de la ECU permite una seguridad más efectiva, pero también tiene beneficios en las etapas de ensayo y fabricación. Cuando las claves públicas para el esquema de firma digital de la ECU están fijadas en la ECU, esto puede provocar dificultades durante el ensayo y en algunas etapas de la fabricación, cuando puede resultar deseable realizar cambios en el software de la ECU o variar los parámetros de la ECU. Cuanto más seguro sea el almacenamiento de claves públicas dentro de la ECU, más problemática resultará esta estrategia durante el ensayo y la fabricación. Entregando el control sobre los valores de la clave pública al inmovilizador se resuelve este problema, ya que el inmovilizador no estará generalmente conectado al sistema hasta que la ECU esté completa. El ensayo y las etapas iniciales de la fabricación pueden tener lugar sin la presencia de un inmovilizador, dotando a los desarrolladores de más libertad para realizar modificaciones. Realizaciones de la invención pueden por lo tanto utilizarse para proporcionar una seguridad mejorada mediante el uso cooperativo del inmovilizador y la ECU, evitando ataques basados en la subversión o la sustitución de la ECU.

En la estrategia descrita aquí, el inmovilizador sirve como certificado raíz de confianza para la ECU, y es utilizado para autenticar recursos digitales en la forma de valores de datos estáticos utilizados por la ECU tales como parámetros del proceso de validación de la ECU. El propio proceso de validación de la ECU puede implicar un proceso de autenticación, formando un árbol de confianza que se extiende desde el inmovilizador a través de la ECU hasta recursos físicos y digitales adicionales.

El inmovilizador también puede utilizarse para servir como certificado raíz de confianza para otros dispositivos informáticos dentro de un vehículo (tales como equipamiento de comunicaciones móviles y dispositivos digitales multimedia) y puede proteger diferentes tipos de recursos digitales (software, parámetros de calibración, medios digitales, parámetros biométricos y cualquier otra forma de datos codificados digitalmente). Esto requiere un camino de comunicación apropiado entre el otro dispositivo informático y el inmovilizador, y requerirá también generalmente de un mecanismo apropiado, tal como un algoritmo de validación de firma digital, en este dispositivo informático para comprobar que el recurso digital no ha sido puesto en riesgo antes de su uso.

REIVINDICACIONES

1.- Un método para hacer seguro un vehículo, que comprende:

proporcionar una unidad (2) de control de motor, donde un elemento de datos digitales estáticos o más de uno se almacenan en una primera memoria (6, 25) para ser utilizados por la unidad (2) de control de motor; y

proporcionar un inmovilizador (3), donde el inmovilizador (3) proporciona un certificado raíz de confianza para la unidad (2) de control de motor y donde el inmovilizador (3) está adaptado para asegurar que el elemento o los elementos almacenados en la primera memoria (6, 25) están protegidos contra una modificación no autorizada;

donde la unidad (2) de control de motor está adaptada para impedir el funcionamiento, o para limitar el rendimiento, de un vehículo a no ser que se lleve a cabo de manera satisfactoria una rutina de validación, donde el mencionado elemento o los mencionados elementos comprenden elementos de datos estáticos utilizados por la rutina de validación y donde los mencionados elementos de datos estáticos comprenden un conjunto de una clave pública o varias de una pareja de claves o un conjunto de claves, donde la clave pública o las claves públicas se utilizan en la rutina de validación para determinar si los valores medidos del software de la unidad de control de motor corresponden a los valores firmados utilizando una clave privada asociada o varias.

2.- Un método según la reivindicación 1, donde el inmovilizador (3) comprende la primera memoria (25), de modo que si se lleva a cabo un intento de modificar o eliminar datos en la primera memoria (25), el inmovilizador (3) proporciona una respuesta de inmovilización para evitar el funcionamiento efectivo del vehículo.

3.- Un método según la reivindicación 2, donde el elemento o los elementos están almacenados en una forma encriptada y/o la memoria (25) del inmovilizador está protegida físicamente contra su modificación.

4.- Un método según la reivindicación 1, donde la primera memoria (6) está comprendida dentro de la unidad (2) de control de motor, y donde el inmovilizador (3) comprueba la primera memoria (6) para determinar si un valor del elemento o los elementos almacenados en su seno son válidos, de modo que si cualquier valor resulta no ser válido, el inmovilizador (3) proporciona una respuesta de inmovilización para evitar el funcionamiento efectivo del vehículo.

5.- Un método según la reivindicación 4, donde la primera memoria (6) está comprendida dentro de una memoria flash de la unidad (2) de control de motor.

6.- Un método según la reivindicación 4 o la reivindicación 5, donde el elemento o los elementos están almacenados en forma encriptada y son desencriptados mediante interacción con el inmovilizador (3).

7.- Un método según cualquier reivindicación precedente, donde el mencionado elemento o los mencionados elementos comprenden un código para ser ejecutado en un procesador de la unidad (2) de control de motor o valores estáticos de la unidad (2) de control de motor o ambos.

8.- Un sistema de control de motor para un vehículo, que comprende:

una unidad (2) de control de motor, donde un elemento o más de uno de datos digitales estáticos se almacenan en una primera memoria (6, 25) para ser utilizados por la unidad (2) de control de motor; y

un inmovilizador (3), donde el inmovilizador (3) proporciona un certificado raíz de confianza para la unidad (2) de control de motor y donde el inmovilizador (3) está adaptado para asegurar que el elemento o los elementos almacenados en la primera memoria (6, 25) están protegidos contra una modificación no autorizada;

donde la unidad (2) de control de motor está adaptada para restringir el funcionamiento del vehículo a no ser que se lleve a cabo de manera satisfactoria una rutina de validación, donde el mencionado elemento o los mencionados elementos comprenden elementos de datos estáticos utilizados por la rutina de validación, y donde los mencionados elementos de datos estáticos comprenden una clave pública o varias de una pareja de claves o un conjunto de claves, donde la clave pública o las claves públicas se utilizan en la rutina de validación para determinar si los valores medidos del software de la unidad de control de motor corresponden a los valores firmados utilizando una clave privada asociada o varias.

9.- Un sistema de control de motor según la reivindicación 8, donde la primera memoria (25) está comprendida dentro del inmovilizador (3).

10.- Un sistema de control de motor según la reivindicación 8, donde la primera memoria (6) está comprendida dentro de la unidad (2) de control de motor, y donde el inmovilizador (3) está adaptado para comprobar la primera memoria (6) para determinar si un valor de la clave pública almacenada en su seno es válida, de modo que si el valor no resulta ser válido, el inmovilizador (3) está adaptado adicionalmente para proporcionar una respuesta de inmovilización para evitar el funcionamiento efectivo del vehículo.

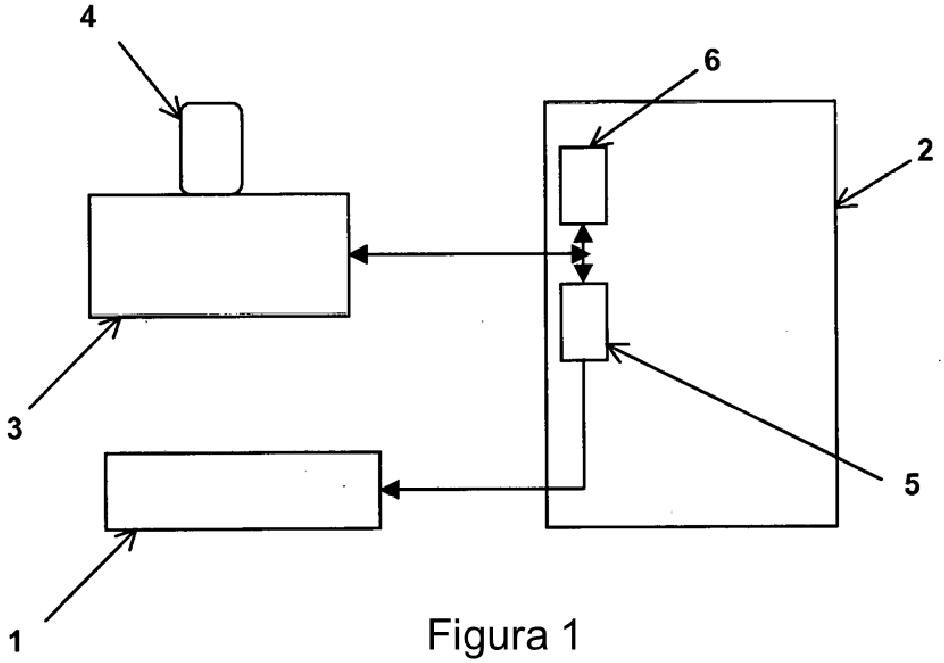

Figura 1

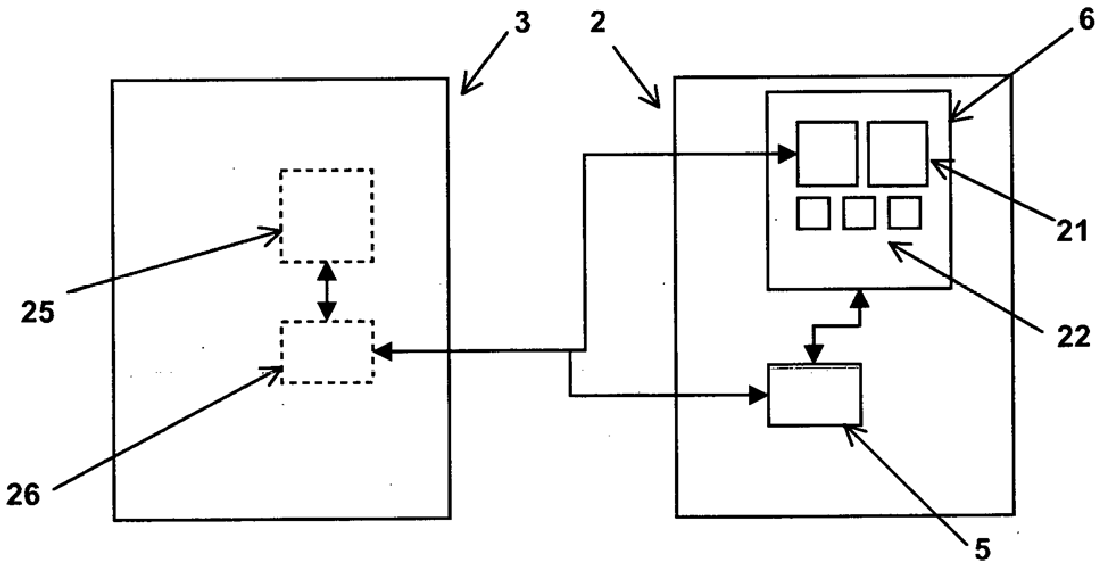

Figura 2

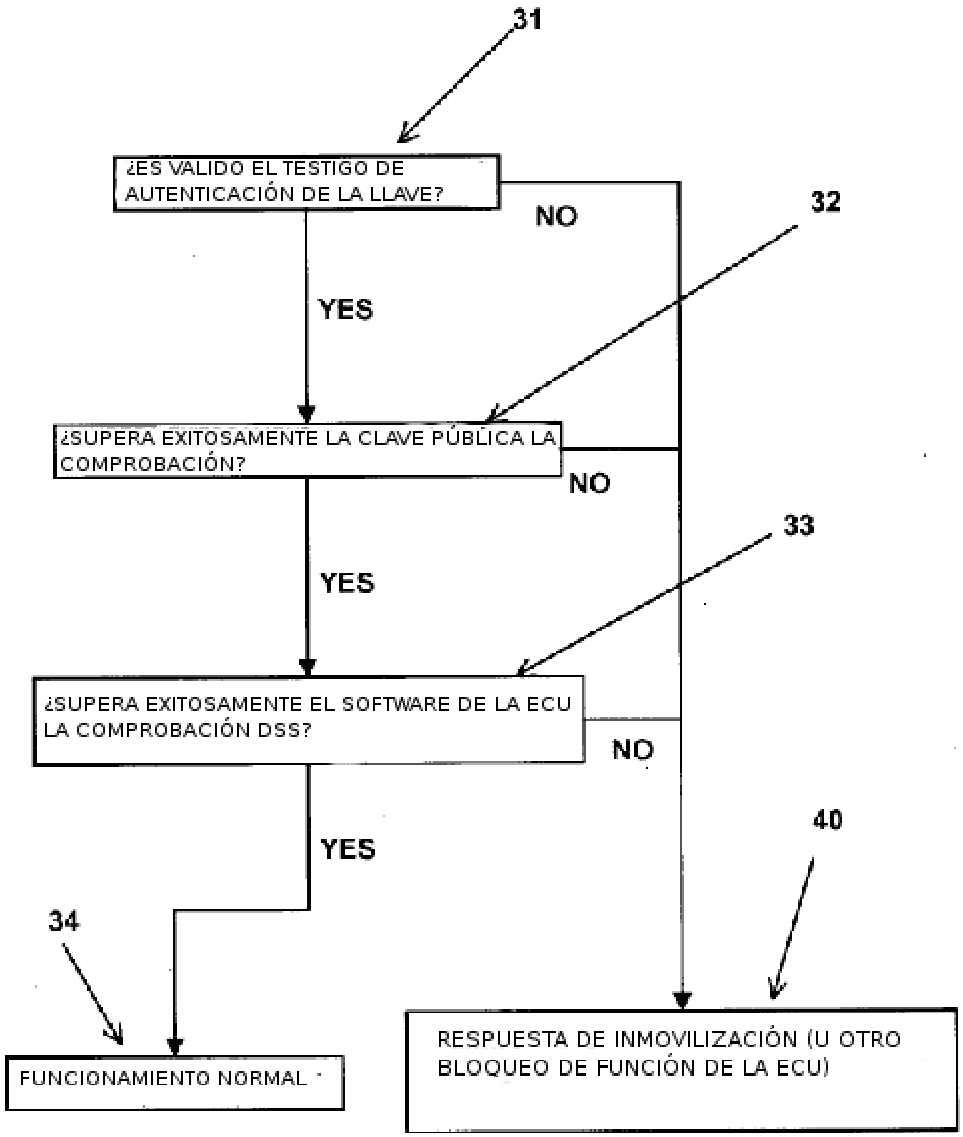
31
¿ES VALIDO EL TESTIGO DE AUTENTICACIÓN DE LA LLAVE?
NO
YES
32
¿SUPERA EXITOSAMENTE LA CLAVE PÚBLICA LA COMPROBACIÓN?
NO
YES
33
¿SUPERA EXITOSAMENTE EL SOFTWARE DE LA ECU LA COMPROBACIÓN DSS?
NO
YES
40
34
FUNCIONAMIENTO NORMAL
RESPUESTA DE INMOVILIZACIÓN (U OTRO BLOQUEO DE FUNCIÓN DE LA ECU)

Figura 3